Secure&Auditable

Hart InterCivic's eSlate™ Solution offers a value-rich, multifaceted architecture that provides the most secure electronic voting system environment in the industry.

Safeguards Against Unauthorized Access

The eSlate System includes both physical and electronic intrusion detection controls, such as standard election seals and time-stamped transaction logs that record every system action related to the voting process. The eSlate System features a secure, real-time embedded operating system that is not Windows-based and therefore not penetrable using common hacker tools. Data cannot be altered or changed by unauthorized personnel because the database structure is proprietary and is protected by encrypted passwords. The election officials in each jurisdiction control these passwords.

No Means of External Access

Each eSlate is activated by the voter using a randomly generated four-number code; there are no smart cards or other programmable devices that create a security breach in the system to provide access for creative hackers or others seeking to tamper, subvert, or vandalize the system or the election. eSlate voting units used in elections are not connected to any external network, so there is no opportunity for someone to access the system remotely and alter code.
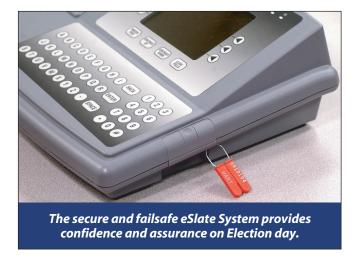
Clear Audit Trail

All components of the eSlate System create an audit record anytime they are accessed or information is changed. All audit records can be extracted and printed in hard copy. All audit reports, audit trail documents, databases, and final reports may be archived in hard copy and/or saved electronically to CD-ROM as needed.

No Reprogramming for Each Election

Unlike punch card and optical scan systems, the system is not reprogrammed with new code for each election; only the election data changes. This eliminates a major source of potential error or manipulation.

Designed for Failsafe Operation

All information managed by the voting equipment is saved in three physically separate devices, providing back-up and redundant data storage in the event any one of the components malfunctions. This is a significant advantage over stand-alone systems that may lose cast votes as a result of a malfunction. Automatic creation of triplicate original cast vote records throughout the course of the day eliminates need to collect votes from each machine upon poll closing, eliminating a potential source

The secure and failsafe eSlate System provides confidence and assurance on Election day.

of error. The eSlate equipment has 18-hours of battery backup to protect against power failures and lost data. All information storage devices are solid-state, and thus are not susceptible to magnetic fields, abusive handling or loss of power.

Integrated Diagnostics and Internal Controls

All data blocks or elements use error-checking techniques to ensure the accuracy of reading and writing digital data. Cyclic data integrity checks ensure that only authorized systems are communicating on the local network, and that the data being communicated originates from a source that has complete integrity with the election database generated by the Ballot Origination Software System™ (BOSS).

The eSlate System software employs user entry validation, real-time error checking, and Cyclic Redundancy Checks (i.e., continuous tests of each transfer of data within a system to ensure that the data received at the end of the transfer are the same as the data originated by the source) incorporated for data-write operations to avoid errors. The system also provides for independent reconciliation of the number of votes cast.

You vote. It counts.™

HART *intercivic*™

800.223.HART · www.hartintercivic.com